BY THE ORDER OF THE COMMANDER
452ND AIR MOBILITY WING

AIR FORCE INSTRUCTION 31-401
MARB Supplement 1
8 November 2000

Security

INFORMATION SECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

Supersedes MARBI 31-401 2 Mar 1998 — Pages 13/Distribution: F

OPR: 452 SFS/SFA (Juanita Perry) — Certified by: 452 AMW/CC (Col Peter T. Bentley)

The OPR for this supplement is 452 SFS/SFA (Juanita Perry). This supplement implements the requirements of DoD 5200.1-R, *Information Security Program Regulation*, AFPD 31-4, *Information Security*, AFI 31-401/AFRC Supplement, *Managing the Information Security Program.* This supplement applies to all 452 AMW and MARB Security Managers. It does not apply to the 163 ANG.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed. This revision requires ISPM to conduct security manager meetings on a quarterly basis (para **1.3.4.4. (Added)**); send letters to unit commander/staff agency chiefs when the primary security manager has one unexcused absence (para **1.3.4.5. (Added))**; require letters be sent to 452 AMW/CC when primary security manager has two or more unexcused absences (para **1.3.4.6. (Added))**; require the appointment of the primary security manager to be either a full time civilian or an Air Reserve Technician (para **1.3.5.1.1. (Added));** Traditional reservists will not be the point of contact for the unit's security program (para **1.3.5.1.1. (Added))**; ensure newly appointed security managers complete the Security Manager Training within two months of appointment (para **1.3.5.2.);** require ISPM to issue a "certificate of training" upon completion of mandatory training (para **1.3.5.2.);** attendance at quarterly security manager meetings is mandatory (para **1.3.6.4.**); Only the ISPM can excuse security managers from attending the quarterly meeting (para **1.3.6.4.);** require a master safe listing for your unit be provided to ISPM NLT 30 Jan of each year (para **1.3.6.13. (Added));** ensure assigned personnel received security education and awareness training in accordance with Annual Training Plan (Part 1) and (Part 2), the Initial Training Plan, and the Unclassified Security Handbook (para **1.3.6.14. (Added));** 452 SFS/SFA will conduct no-notice ISPOVs (para **1.4.2.**); units/staff agencies with unsatisfactory rating will be revisited within 90 days to ensure observations have been corrected (para **1.4.2.1. (Added)**); units/staff agencies with classified material will conduct semiannual security self-inspections, not later than 15 Mar and 15 December (para **1.4.3.1.2. (Added));** TSCOs are required to read and complete the 452 SFS/SFA TSCO Training Handbook within 30 days of appointment (para **5.10.1.1.4. (Added));** an 80% must be obtained for a passing score (para **5.10.1.1.4. (Added));**

ensure users do not leave a FORTEZZA card in an unattended terminal (para **5.12.2. (Added));** for incidents involving loss, theft, or tampering of FORTEZZA cards contact the Certification Authority (452 CS/SCBS) (para **5.12.7. (Added));** post storage facility approval letter immediately inside the approved area along with a copy of the facility written procedures (para **5.20.1.**); training must be conducted within 30 days for cleared (with access) individuals and 60 days for uncleared (without access) individuals; (para **8.3.1.1. (Added));** the Initial Security Training Handbook developed by the ISPM will be used to brief each individual (para **8.3.1.1. (Added));** security managers will provide initial training to newly assigned personnel (para **8.3.1.2. (Added));** upon completion of the briefing, individuals will sign the checklist (para **8.3.1.2. (Added));** all training will be documented using the "Security Education and Training Program Log" or a similar log for all cleared personnel (para **8.3.1.3. (Added));** security managers must ensure this training is accomplished (para **8.9.1. (Added)**); Annual Training Handbook (Part 1) will be used during the period of 1 Jan – 30 Jun (para **8.9.1. (Added));** Annual Training Handbook (Part 2) will be used during the period of 1 Jul – 31 Dec (para **8.9.1. (Added));** training will be documented using the "Security Education and Training Program Log" (para **8.9.1. (Added));** the log will be maintained in Section 2 of the Security Manager's Handbook (para **8.9.1. (Added));** Uncleared personnel will receive training using the "Unclassified Training" Handbook (para **8.9.2. (Added));** this training is required on an annual basis (para **8.9.2. (Added));** Security managers must be able to document what, how, and when training was provided to personnel (para **8.9.2. (Added));** the investigating official will provide the ISPM a copy of the final report (para **9.3.2.4.)**

AFI 31-401 is supplemented as follows:

1.3.4. The Chief, Security Forces is designated as the Information Security Program Manager (ISPM) for the 452 AMW and delegates ISPM duties to the Chief, Security Forces Administration (SFA). A host tenant agreement with the Air Force Audit Agency, 4th Air Force and 701st Combat Operation Squadron allows the 452 SFS/SFA to process their personnel clearance requests and to conduct oversight reviews. The 163 SFS is the program manager for the 163 ARW. The ISPM will:

1.3.4.4. **(Added)** Conduct security manager meetings on a quarterly basis.

1.3.4.5. **(Added)** Send letters to unit commanders/staff agency chiefs when the primary security manager has one unexcused absence.

1.3.4.6. **(Added)** Send letters to 452 AMW/CC when the primary security manager has two or more unexcused absences.

1.3.5.1.1. **(Added)** The appointment of the primary security manager is either a full time civilian or an Air Reserve Technician (ART). Traditional reservists will not be the point of contact for their unit's security program.

1.3.5.2. Ensure newly appointed security managers complete the Security Manager Training within two months of appointment. Upon completion of the mandatory training, the ISPM will issue a "certificate of training".

1.3.6.1. Maintain a security manager's handbook per direction of 452 SFS/SFA and in accordance with Attachment 12, **Security Manager's Continuity Handbook.** No deviation is permitted. Maintain only the items listed in Attachment 12 in the handbook. Keep the book updated and free of frivolous information.

1.3.6.4. Attend quarterly security manager meetings conducted by the ISPM. Attendance is mandatory. Only the ISPM can excuse security managers from attending the quarterly meeting.

1.3.6.9. **(Added)** Manage the Clearance Access Verification Program (CAVS) roster to include identifying personnel who require a personnel security investigation (PSI). Security managers will print a new CAVS roster every 30-45 days.

1.3.6.10. **(Added)** Notify personnel who have been identified for a periodic reinvestigation (PR) and assist them with completing appropriate forms. Use the Electronic Personnel Security Questionnaire (EPSQ) to submit PSIs to the Personnel Security Section (452 SFS/SFAI) for processing. Ensure all PSI processing is completed within 15 days of initial notification for ARTs and full time government employees. Traditional reservists have three (3) UTA weekends (90 days) for processing their PSIs. ***NOTE:*** Failure to submit required PSIs in a timely manner may jeopardize an individual's security clearance eligibility.

1.3.6.11. **(Added)** Coordinate restricted area badge and AF Form 2586, **Unescorted Entry Authorization Certificates**, issues with Report and Analysis (452 SFS/SPAR). For departing personnel, ensure each restricted area badge is turned in before departure.

1.3.6.12. **(Added)** Update the Entry Authorization Listing as required and return it to 452 SFS/SFAR within 15 days.

11.3.6.13. **(Added)** Develop a master safe listing for your unit and provide a copy to ISPM. This list should contain the following: container ID, location, description, make, model, serial number, year manufactured, X-07/08 combination compliant (YES/NO), and the safe custodian's name, home and duty phone numbers. Submit this listing to ISPM no later than 30 Jan of each year.

1.3.6.14. **(Added)** Ensure assigned personnel receive security education and awareness training in accordance with Annual Training Plan (Part 1) and (Part 2), the Initial Training Plan, and the Unclassified Security Handbook.

1.4.2. 452 SFS/SFA conducts Information Security Program Oversight Visits (ISPOV) on an annual basis for all units/staff agencies that store classified material. Conduct ISPOVs on all other units/staff agencies on a 24-month basis. 452 SFS/SFA will conduct no-notice ISPOVs.

1.4.2.1. **(Added)** Provide ISPOV reports to each commander/staff agency chief and break down by observations, recommendations, and summary. Provide a copy of each ISPOV report to 452 AMW/CC. Units/staff agencies with unsatisfactory rating will be revisited within 90 days to ensure observations have been corrected.

1.4.2.2. **(Added)** During ISPOVs, the ISPM may identify personnel for the "beyond compliance award". This award is given in the form of a Commendation Letter to those who demonstrate the ability to go beyond compliance with Information and Personnel Security directives.

1.4.3.1.1. **(Added)** Unit Commanders and staff agencies involved with processing or holding classified information ensure personnel conduct semiannual security self-inspections to evaluate information security program effectiveness.

1.4.3.1.2. **(Added)** Units/staff agencies with classified material will conduct semiannual security self-inspections, not later than 15 Mar and 15 December. Send a letter to ISPM no later than 10 days after the completion of the self-inspection stating that a self-inspection was completed, along with the findings/deficiencies and proposed corrective actions. The security manager will monitor the self-inspection program and follow-up on all findings/deficiencies to ensure they are corrected.

1.4.3.1.3. **(Added) Security Manager of the Year Award.** At the end of the calendar year, the ISPM will select a security manager whose Personnel and/or Information Security Programs are rated as "Best of the Year". The award will be presented at the December Quarterly Security Manager meeting.

2.1.1. The Commander, 4AF, has been designated as a Secret OCA. The authority to originate classified information is exercised sparingly and only when no promulgated classification guidance exists.

2.4.5. **(Added)** An action officer who develops information that is currently not classified under a security classification guide and believes the information warrants safeguarding, routes the information to 4AF/CC for classification evaluation. The action officer is responsible for advising 452 SFS/SFA and the unit security managers of the OCA classification decision.

3.1. Direct any questions concerning declassifying and downgrading information to 452 SFS/SFA.

4.1. The originator of classified information is responsible for proper application of classification markings. This includes derivative classification decisions and working papers. Those who prepare derivative classified documents will first review Executive Order 12958, DoD 5200.1-PH, *DoD Guide to Marking Classified Documents.*

4.4.1. **(Added)** Refer complex marking issues to the security managers or 452 SFS/SFA for assistance.

5.10.1.1.3. **(Added)** Decontrol the preceding year's TS register no later than 15 January each year.

5.10.l.1.4. **(Added)** TSCOs are required to read and complete the 452 SFS/SFA TSCO Training Handbook Test within 30 days of appointment. Obtain an 80% for a passing score. Issue a certificate of training upon completion.

5.10.1.1.5. **(Added)** Personnel are not permitted to work alone in areas where this information is used, stored, or accessible.

5.12. Each unit commander/staff agency chief responsible for storing and/or processing classified (also recommended for all other agencies) establishes a system for end-of-day (duty day) security checks to be conducted within their area of responsibility. This ensures that all classified material is stored in the security container and the security container is locked at the end of the duty day. It is recommended each unit/staff agency implement a clean desk policy to aid in the accomplishment of the end-of-day check.

5.12.1. **(Added)** Post a letter identifying personnel who are authorized to conduct end-of-day check for each unit/staff agency. Personnel assigned this task will receive training/briefings by the security managers on the proper procedures.

5.12.2. **(Added)** End-of-day checks should include desktops, file baskets, cabinet tops, trash containers, fax machines, etc. for the presence of classified materials. Check all reproduction machines and shredders. Check all stand-alone Emission Security (EMSEC) approved information systems, secure telephone units (STU-III) and any secure data fax machines for proper storage of the crypto ignition keys. Ensure users do not leave FORTEZZA cards in an unattended terminal. Secure the card in a GSA-approved container within the office, or if not available, a locked drawer or cabinet that is not located in the same room as the STU-III.

5.12.3. **(Added)** Before leaving the area, all employees should ensure all classified notes, carbon paper, classified typewriter ribbons, rough drafts, and similar papers are placed in storage containers to assist in the end-of-day checks.

5.12.4. **(Added)** Rotate the combination dial of each container at least (4) times in one direction to assure locked condition of the container. This procedure does not apply to electronic (X-07/X-08) security locks.

5.12.5. **(Added)** After checking SFs 702, **Security Container Check Sheet,** for all assigned security containers and performing inspections of each unit/staff agency office area, complete and sign the SF 701, **Activity Security Checklist.** Indicate the names of personnel working after the end-of-day check and, if applicable, their responsibility for security of a particular container. Enter the time of the inspection and initial the “checked by” column of the SF 701.

5.12.6. **(Added)** If designated personnel discover unattended classified, they should report it immediately to the Command Post and unit/staff agency security manager. Secure the classified in the Command Post or a unit/staff agency safe until the next duty day. The security manager must contact the ISPM the next duty day.

5.12.7. **(Added)** For incidents involving COMSEC materials, immediately contact the COMSEC manager (452 CS/SCBS) during normal duty hours, or through the 452 AMW Command Post after normal duty hours. For incidents involving loss, theft, or tampering of FORTEZZA cards contact the Certification Authority (CA) (452 CS/SCBS).

5.15.1.1. **(Added)** Before scheduling classified meetings, contact the ISPM to ensure all security precautions are completed.

5.15.1.2. **(Added)** Unit/staff agency conducting the meeting will appoint a security OPR for the meeting. This responsibility is normally given to the unit security manager.

5.15.1.3. **(Added)** A classified meeting checklist is available from the ISPM.

5.15.1.4. **(Added)** Ensure all personnel have the appropriate level of clearance eligibility before starting the meeting. Clearance Access Verification System (CAVS) roster, visit request letters, and TDY orders are acceptable for this purpose. The use of restricted area badges as meeting eligibility criteria is prohibited. Contact 452 SFS/SFAI for assistance in obtaining a copy of the CAVS roster.

5.15.2. **Approval Authority.** The ISPM will assess the need to set up and approve secure conference facilities.

5.20.1. The ISPM will approve in writing facilities used for open/unattended storage of classified (Secret and Confidential). Facilities must have strict written procedures. Post storage facility approval letter immediately inside the approved area along with a copy of the facility written procedures. Contact the ISPM for further guidance.

5.20.2. Offices storing small numbers of classified documents that do not warrant an entire security container (approved GSA safe) may request courtesy storage from another office. Maintain a letter of agreement between the two offices in the safe with the documents. Separate the documents from the safe contents by placing them in a sealed envelope/container.

5.20.2.1. **(Added)** The 452 AMW Command Post has been designated as a repository for overnight temporary storage of in-transit classified materials.

5.23.2.1. **(Added)** The first person listed on the SF 700, **Security Container Information**, is considered the primary safe custodian. The SF 700 will also list all personnel who possess the safe combination. Safe custodian responsibilities:

5.23.2.2. **(Added)** Change safe combinations at required intervals.

5.23.2.3. **(Added)** Combinations are changed when placed in use; whenever an individual knowing the combination no longer requires access; when the combination has been subject to compromise; at least every 2 years; or when taken out of service.

5.23.2.4. **(Added)** For special access programs refer to the appropriate directive for required intervals.

5.23.2.5. **(Added)** Report container malfunctions to the 452 CES customer service desk.

5.23.2.6. **(Added)** Ensure all documents placed in the safe are properly marked.

5.23.2.7. **(Added)** Identify safe contents on unit/staff agency file plans.

5.23.2.8. **(Added)** Store TS documents, to include TS working papers, at the Top Secret Control Account (TSCA) within the 452 AMW Command Post. Contact 452 SFS/SFA for guidance.

5.23.2.9. **(Added)** Storage of any other special access required classified information. Consult with the cognizant security OPR for the special access program on unique storage requirements before storing such documents at March ARB. Contact 452 SFS/SFA for security OPRs.

5.29.2.5.1. **(Added)** Process classified for destruction as soon as classified has served its purpose.

5.29.2.5.2. **(Added)** Destroy unnecessary classified on a monthly basis to preclude accumulation.

5.29.2.5.3. **(Added)** Destroying unnecessary classified prevents the need for additional storage containers, requires less accountability, and prevents potential security violations.

5.29.2.5.4. **(Added)** All areas containing and storing classified material will obtain an approved device for destroying classified documents. For a list of approved devices, see Air Force Table of Allowances (TA) 006, *Organizational and Administrative Equipment.*

5.29.2.5.5. **(Added)** Records Management (452 CS/SCBR) will be the Base Central Destruction Facility (BCDF). 452 CS/SCBR will properly train personnel to use the BCDF. Units needing to destroy non-document type of classified waste (plastic, microfiche, tapes, etc.) will coordinate with 452 CS/SCBR for destruction.

5.29.2.5.6. **(Added)** Classified wastes, leaving the base or work area, will be controlled as stated in Chapter 6 for transmitting classified materials.

5.31. **(Added) Annual Clean-out Week.** The Annual Clean-Out Week is the first week of August. Each commander/staff agency chief responsible for maintaining and storing classified material must appoint a safe custodian to review all classified material for destruction. Commanders/staff agency chiefs will provide 452 SFS/SFA a written report stating that a review was conducted and all unnecessary classified was identified and destroyed. Include in this report the approximate amount of classified destroyed. EXAMPLE: "half a drawer"; "one drawer"; "one manual", etc. The report is due annually to 452 SFS/SFA no later than **15 Aug**.

6.1.1.l. **(Added)** 452 CS/SCBA is responsible for processing incoming and outgoing classified distribution (first class "*Do Not Forward"*, registered, and certified mail). Transportation Management Office (TMO) is responsible for processing incoming and outgoing classified that will be shipped through Federal Express mail.

6.1.2.l. **(Added)** 452 CS/SCBA or any unit that receives, first class *"Do Not Forward"*, registered, certified, or Federal Express mail will protect it as classified information until opened. Classified will then be stored within an approved security container.

6.1.3.l. **(Added)** Personnel who are sending or receiving classified materials through Federal Express mail are cautioned that Federal Express delivers directly to the addressee. Sender must ensure that the material is delivered to personnel with the appropriate clearance and who have the ability to protect the material.

6.1.5. **(Added)** Commanders/staff agency chiefs or supervisors approve appropriately cleared personnel to remove classified information from the work area for the following purposes:

6.1.5.1. **(Added)** Routine destruction at the Base Central Destruction Facility (BCDF) or at a designated area/facility.

6.1.5.2. **(Added)** For official duties on March ARB or for hand-carrying classified documents to off-base areas under the control of the Installation Commander accomplish the following: Obtain permission from the commander/staff agency chief or supervisor to remove/pick-up classified material from the workplace. Attach a SF 704, **Secret Cover Sheet,** or SF 705, **Confidential Cover Sheet;** enclose the material in an outer container such as a sealed envelope, folder (closed with a lock, tie, or Velcro), briefcase, zippered bag, etc. ***NOTE:*** Classified markings must not appear on the outer container. Individuals must possess written authorization on a DD Form 2501, **Courier Authorization.** The security manager will issue and maintain DD Forms 2501.

6.1.5.3. **(Added)** Aircrew may carry classified material in brown attaché cases, clearly marked on the outside with red tape marked SECRET on it. This practice is only allowed to and from the aircraft.

6.1.6. **(Added)** For removal of classified documents from March ARB to off-base areas not under the control of the Installation Commander, the following procedures will apply:

6.1.6.1. **(Added)** For transmission off the installation see DoD 5200.1-R.

6.1.6.2. **(Added)** Personnel authorized to remove classified information must be briefed on their responsibilities for protection of classified by their security manager or supervisor.

6.1.6.3. **(Added)** Additional written authorization is required when traveling by aircraft. Consult with your security manager and information security directive listed above.

6.1.7. **(Added)** 452 SFS will conduct random entry point inspections to deter unauthorized removal of classified from the installation. Personnel hand-carrying classified documents to off-base areas are required to be in possession of courier authorizations and exemptions notices any time classified information is carried through an entry point.

7.1.1. Direct any questions concerning Special Access Programs to 452 SFS/SFA.

8.1.2. The ISPM will train security managers within two months of appointment.

8.3.1.l. **(Added)** Conduct training within 30 days for cleared (with access) individuals and 60 days for uncleared (without access) individuals. The "Initial Security Training Handbook" developed by the ISPM will be used to brief each individual. Maintain a copy of the "Initial Training Checklist for New Personnel" on each newly assigned individual.

8.3.1.2. **(Added)** The unit security manager will provide initial training to newly assigned personnel. Upon completion of the briefing, individuals will sign the checklist. File the checklist in Section 2 of the Security Manager's Handbook.

8.3.1.3. **(Added)** Use the "Security Education and Training Program Log" or a similar log, to document training for all cleared personnel .

8.9.1. **(Added)** Security managers must ensure this training is accomplished. Conduct training semiannually for cleared personnel. Use the Annual Training Plan (Part 1) Handbook during the period of 1 Jan – 30 Jun. Use the Annual Training Plan (Part 2) Handbook the period 1 Jul – 31 Dec. Use the "Security Education and Training Program Log", contained in the Security Manager's Training Handbook to document training. Maintain this log in Section 2 of the Security Manager's Handbook.

8.9.2. **(Added)** Use the "Unclassified Training" Handbook to train uncleared personnel. This training is required on an annual basis. It is not necessary that individual's training be documented using the "Security Education and Training Program Log". However, security managers must document what, how, and when training was provided to personnel.

9.2.6.1. **(Added)** Anyone who knows or believes there may have been a compromise, possible compromise, loss, unauthorized disclosure, or other infraction affecting the integrity of classified information must report it without delay to his or her security manager. The unit security manager contacts the ISPM for further guidance. The ISPM assigns a case number beginning with the calendar year, base, and sequential number for tracking purposes.

9.3.2.1. The commander/staff agency chief of the unit or agency where the violation occurred is the appointing authority and appoints a disinterested Noncommissioned Officer (E-7 or above), a commissioned officer or a civilian employee (GS-07 or above) to conduct inquiries or investigations into the events surrounding security violations. The investigating official will not be assigned to the same division/branch where the suspected incident took place. Forward a copy of the appointment letter to 452 SFS/SFA.

9.3.2.3. Upon being appointed, the investigative official reports to the ISPM for a briefing.

9.3.2.4. **(Added)** Investigation officials coordinate their actions with the ISPM. The investigating official will provide the ISPM a copy of the final report.

9.3.2.5. **(Added)** Complete inquiry reports within 10 workdays and investigation reports within 30 workdays.

9.4.1.4. The ISPM will retain a copy of the investigation.

PETER T. BENTLEY, Colonel, USAFR
Commander

ATTACHMENT 12 (Added)
SECURITY MANAGER'S HANDBOOK TABLE OF CONTENTS

1. Appointment Letters (Keep the most current letters)

Primary & Alternate Security Managers/Monitors

Primary & Alternate TSCOs (if applicable)

Primary & Alternate Safe Custodians (if applicable)

Personnel Authorized to Reproduce Classified (if applicable)

Personnel Authorized to Pick-up/Receipt for FedEx, Registered, First Class, & Express Postal

2. Training Material (Keep until superseded or rescinded)

Unit/Staff Agency Information Security Operating Instructions

Open Storage Instructions

Training Certificate (s)

Security Education Training Log

Semiannual Training Handbook, Part 1 (classified accounts only)

Semiannual Training Handbook, Part 2 (classified accounts only)

Unclassified Account Training Handbook (if applicable)

Security Manager's Training Handbook

Initial Training Handbook

Initial Training Completed Checklists

Courier Briefing Handbook (if applicable)

Courier Briefing Certification (if applicable)

3. Semiannual Self-Inspection (SI) Program (Keep all copies until next ISPOV)

Self-Inspection Appointment Letters

SI Checklists (HQ AFRC/SFI Checklist Only)

SI Reports and Replies

4. Top Secret Inventory Report (if applicable)

5. Information Security Program Oversight Visit (ISPOV) Reports
(Keep the last two)

6. Information/Personnel Security Program Miscellaneous Information
(Keep for one year)

Quarterly Security Manager's Meeting Minutes

Personnel & Information Security Newsletter

452 SFA Letters/Instructions

7. Unit/Agency Clearance Access Verification System (CAVS) (Keep the most current CAVS roster, print every 30-45 days)

CAVS Rosters (PR, SAR, etc.)

Interim Clearances (AF 2583)

Suspense Copies of AF Form 2583 for Personnel Security Investigations

AF Form 2587, **Security Termination Statement** (Keep for two years)

8. Unit/Agency Restricted Area Badge

Restricted Area Badge OI/Procedures

EAL (keep the most current)

Original Copy of AF Forms 2586, **Unescorted Entry Authorization Certificate** (maintain until bearer surrenders the badge)

Phase I/II Training Handbook

Phase I Completed Test

Escort Certification

Escort Test Results

9. Miscellaneous Security Information (Keep for one year)

Correspondence Relating to Sentinel Key/CAVS/EPSQ

Quarterly Security Reports

Other Miscellaneous Security Information